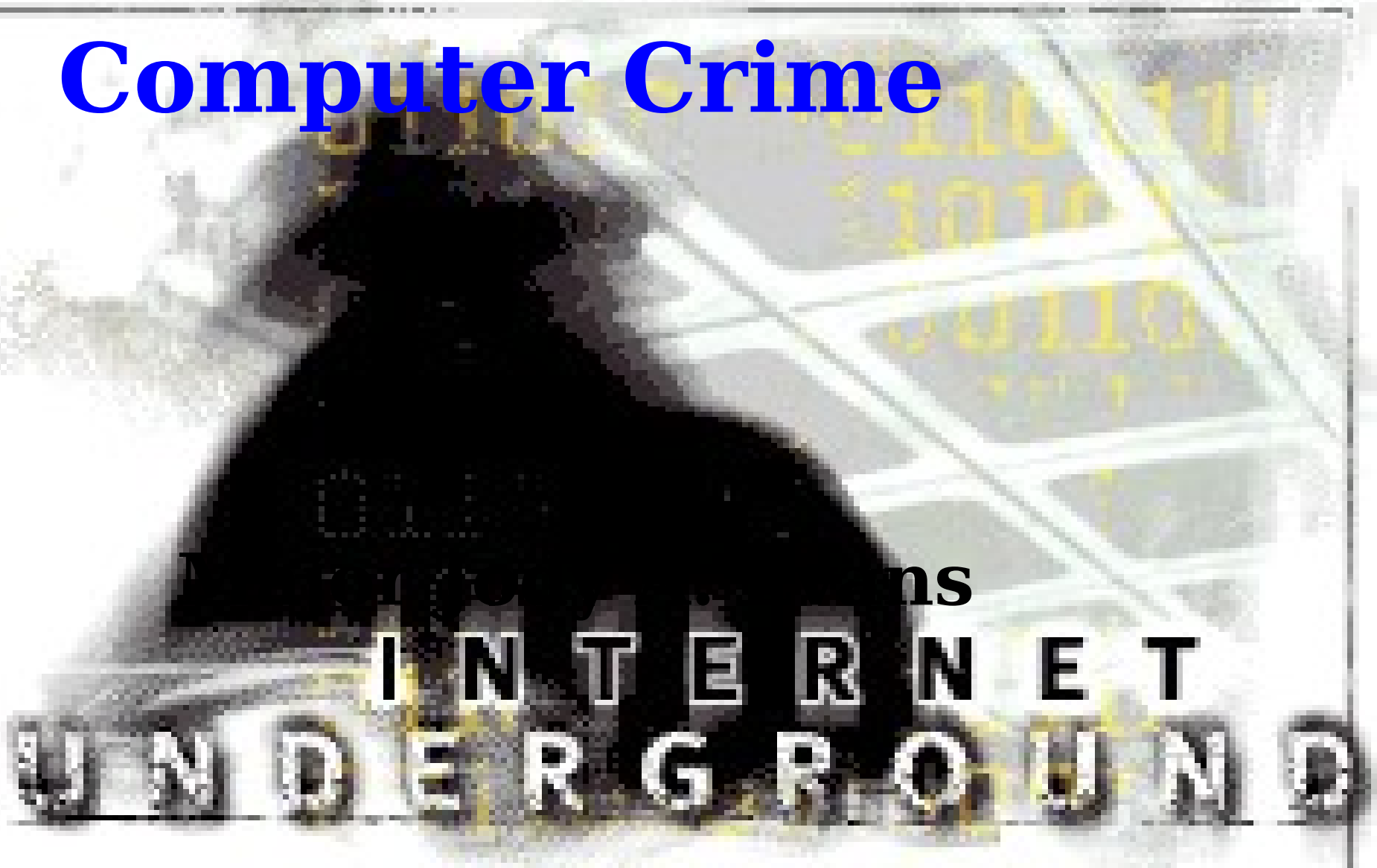
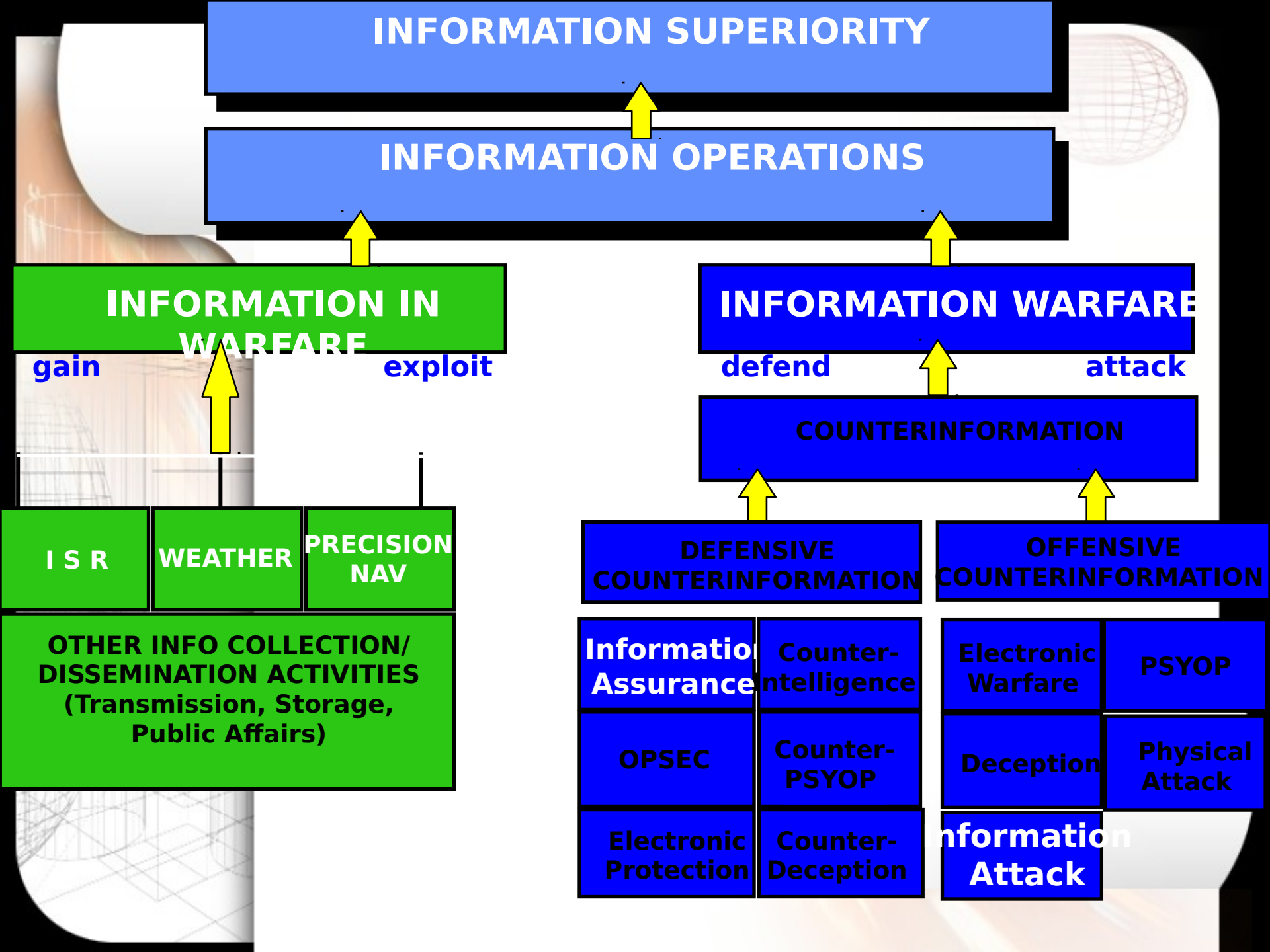
Computer Crime



Overview

- Relationship of Computer Crime
  - (part of IA) to CNA
- The Problem
- Computer Crime Team
- Types of Computer Crime
  - Insider (military v. civilian)
  - Outsider
- Investigations
- Typical Scenarios

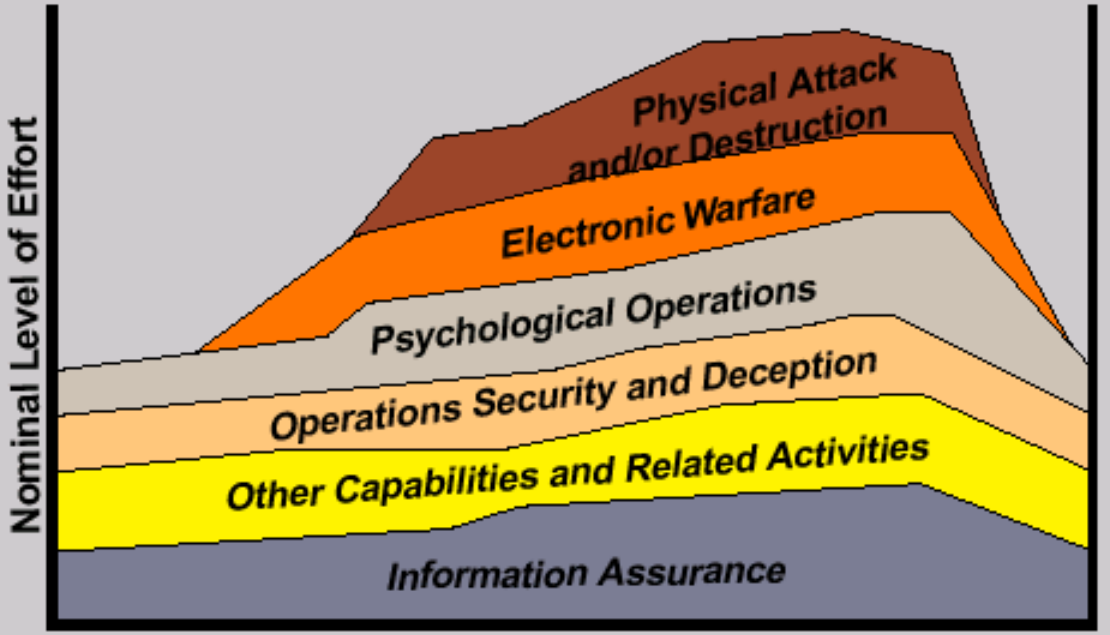

INFORMATION SUPERIORITY
INFORMATION OPERATIONS
INFORMATION IN WARFARE
INFORMATION WARFARE
gain
exploit
defend
attack
COUNTERINFORMATION
I S R
WEATHER
PRECISION NAV
OTHER INFO COLLECTION/ DISSEMINATION ACTIVITIES (Transmission, Storage, Public Affairs)
DEFENSIVE COUNTERINFORMATION
OFFENSIVE COUNTERINFORMATION
Information Assurance
Counter-Intelligence
OPSEC
Counter-PSYOP
Electronic Protection
Counter-Deception
Electronic Warfare
PSYOP
Deception
Physical Attack
Information Attack

Information Assurance

- **Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD S-3600.1)**

Acrobat Reader - [jp3_13.pdf]
File Edit Document View Window Help

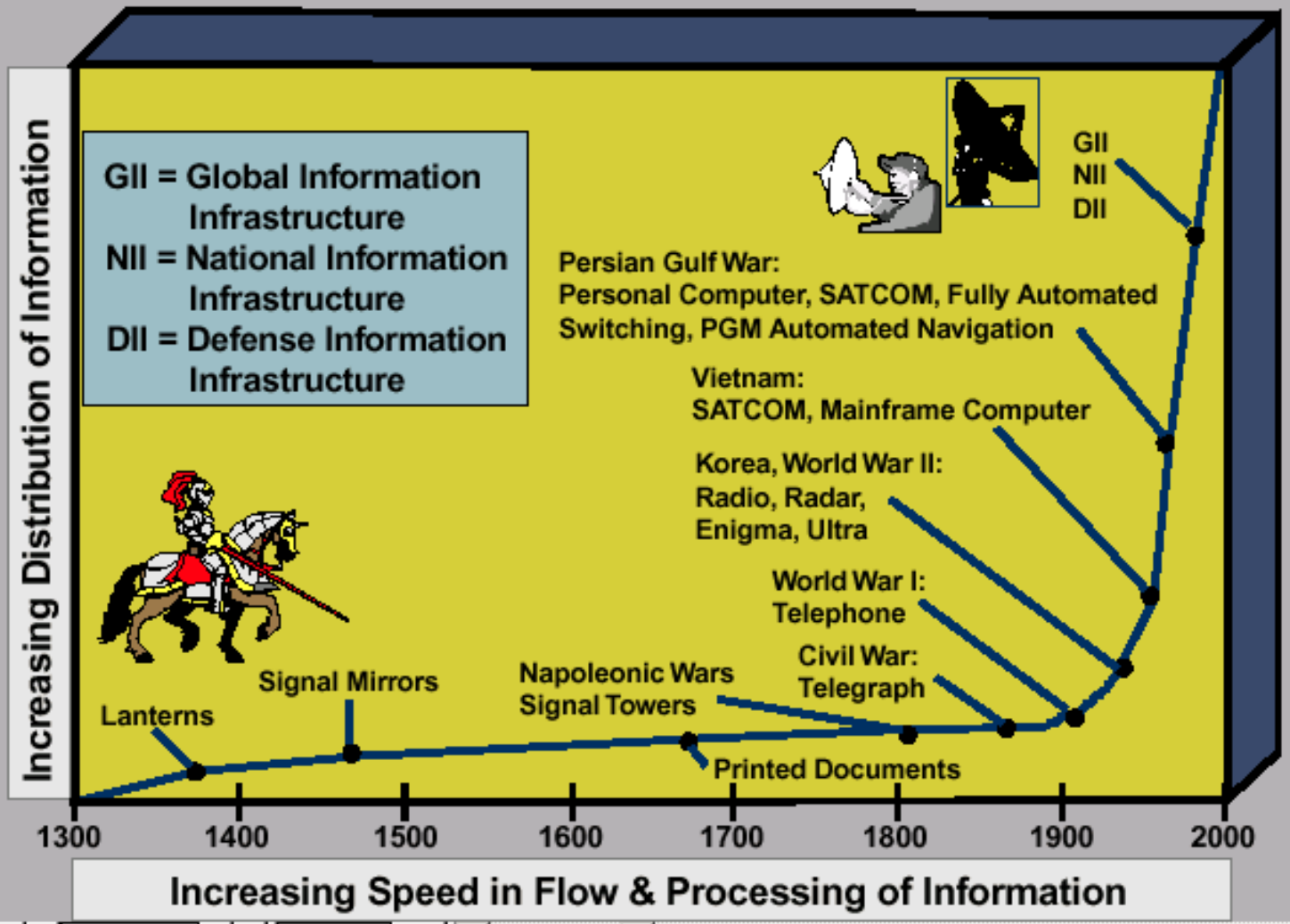
NOTIONAL INFORMATION OPERATIONS ENGAGEMENT TIMELINE



150% 40 of 136 6 x 9 in
Start 12:47 PM

Acrobat Reader - [jp3_13.pdf]
File Edit Document View Window Help

INCREASING ACCESS TO INFORMATION



200% 24 of 136 6 x 9 in
Start 12:40 PM

Recent events ... and *the problem.*

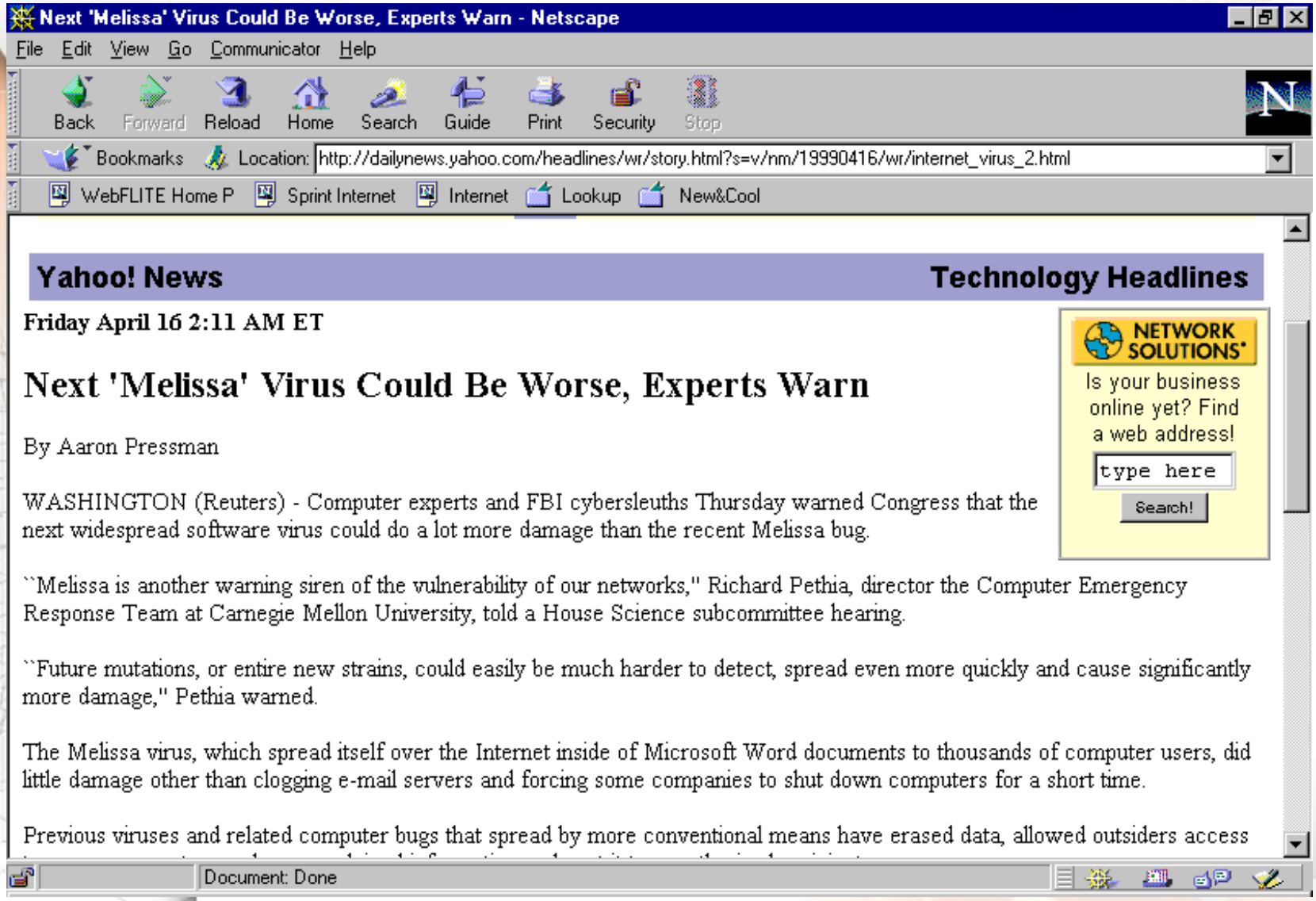
Recent Events

- 1983
  - Pedophiles began using computer bulletin boards to communicate and trade
  - North America Man-Boy Love Association (NAMBLA)
- 1996
  - Nearly 1 million children identified as victims of abuse or neglect
  - 12% victims of sexual abuse

Recent Events

- 2000
  - Recent estimates indicate that over 60 million people worldwide have Internet access
  - Sexual predators use computers and Internet to troll and find victims with minimal risk
  - Traditional security measures (fences, gates, guards) can’t protect from cyber-crime

The Problem


Next 'Melissa' Virus Could Be Worse, Experts Warn - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://dailynews.yahoo.com/headlines/wr/story.html?s=v/nm/19990416/wr/internet_virus_2.html
WebFLITE Home P Sprint Internet Internet Lookup New&Cool
Yahoo! News
Technology Headlines
Friday April 16 2:11 AM ET
Next 'Melissa' Virus Could Be Worse, Experts Warn
By Aaron Pressman
WASHINGTON (Reuters) - Computer experts and FBI cybersleuths Thursday warned Congress that the next widespread software virus could do a lot more damage than the recent Melissa bug.
``Melissa is another warning siren of the vulnerability of our networks,'' Richard Pethia, director the Computer Emergency Response Team at Carnegie Mellon University, told a House Science subcommittee hearing.
``Future mutations, or entire new strains, could easily be much harder to detect, spread even more quickly and cause significantly more damage,'' Pethia warned.
The Melissa virus, which spread itself over the Internet inside of Microsoft Word documents to thousands of computer users, did little damage other than clogging e-mail servers and forcing some companies to shut down computers for a short time.
Previous viruses and related computer bugs that spread by more conventional means have erased data, allowed outsiders access
NETWORK SOLUTIONS
Is your business online yet? Find a web address!
type here
Search!
Document: Done

The Problem

CNN.com - Technology - 'ILOVEYOU' virus threatens commerce, e-mail and

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Netsite: http://cnn.com/2000/TECH/computing/05/04/iloveyou.02/index.html#1 What's Related

Instant Message WebMail Radio People Yellow Pages Download Calendar Channels

MAINPAGE
WORLD
U.S.
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
POLITICS
LAW
TRAVEL
FOOD
ARTS & STYLE
BOOKS
NATURE
IN-DEPTH
ANALYSIS
LOCAL

myCNN
Headline News brief
news quiz
daily almanac

MULTIMEDIA:

'ILOVEYOU' virus threatens commerce, e-mail and history

May 4, 2000
Web posted at: 8:23 p.m. EDT (0023 GMT)

In this story:

'LOVE' already costing much

Senate has no love for 'LOVE'

History nearly lost

How it works

'It's very clever'

RELATED STORIES, SITES

By D. Ian Hopper
CNN Interactive Technology Editor

(CNN) -- Computer users around the world survived a particularly rough day Thursday as the self-propagating and destructive "ILOVEYOU" virus destroyed critical files and jammed electronic mail systems, causing millions of dollars in damages.

Experts estimated that 60 percent to 80 percent of U.S. companies were infected. Additionally, several U.S. government agencies and the Senate were hit, as well as more than 100,000 servers in Europe.

The virus was first reported in Hong Kong and spread gradually west as

CNN Sites
Search
CNN.com
Find

TECHNOLOGY
TOP STORIES

'ILOVEYOU' virus threatens commerce, e-mail and history

Video coming to an IP near you

RIAA CEO talks about legal proceedings against MP3.com and Napster

Astronomers detect universe's missing hydrogen

Feds losing cyberspace race

Interview: The inside scoop on Transmeta's Crusoe chip

(MORE)

CNN.com
TOP STORIES

'ILOVEYOU' virus threatens commerce, e-mail and history

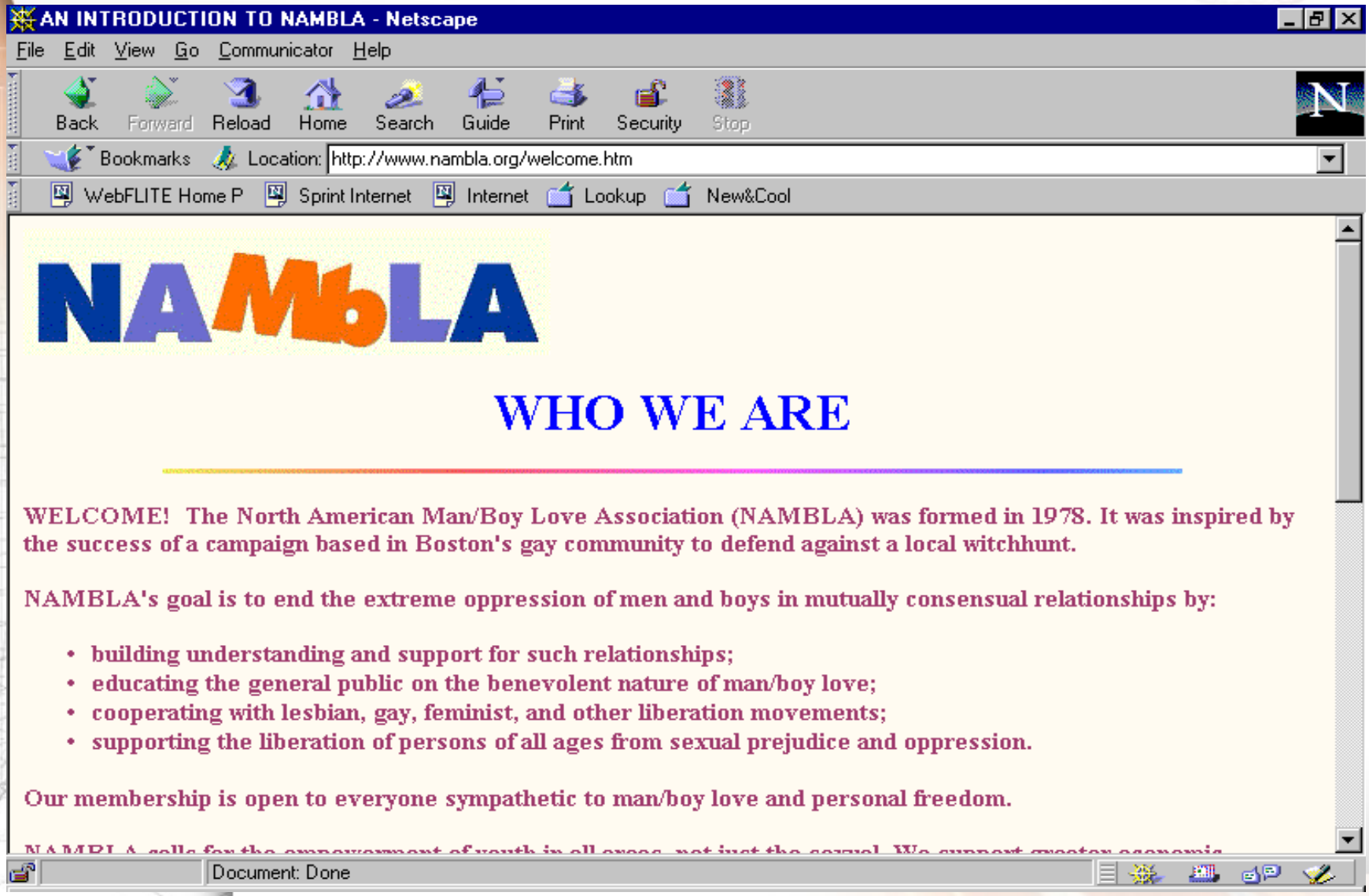
Lockerbie trial begins day 2 with eyewitness accounts of explosion

Pan Am 103 trial could ease

Document: Done

Start CNN.com - Technolo... RE: FW: Stallens ROT - In... Microsoft PowerPoint - [Sa... SnagIt/32 7:48 PM

The Problem


AN INTRODUCTION TO NAMBLA - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.nambla.org/welcome.htm
WebFLITE Home P Sprint Internet Internet Lookup New&Cool
NAMBLA
WHO WE ARE
WELCOME! The North American Man/Boy Love Association (NAMBLA) was formed in 1978. It was inspired by the success of a campaign based in Boston's gay community to defend against a local witchhunt.
NAMBLA's goal is to end the extreme oppression of men and boys in mutually consensual relationships by:
• building understanding and support for such relationships;
• educating the general public on the benevolent nature of man/boy love;
• cooperating with lesbian, gay, feminist, and other liberation movements;
• supporting the liberation of persons of all ages from sexual prejudice and oppression.
Our membership is open to everyone sympathetic to man/boy love and personal freedom.
Document: Done

Presidential Decision Directive 62: Combating Terrorism

- US military superiority + available technology = increasing likely use of:
  - weapons of mass destruction
  - advanced computer technology to attack
    - economy
    - critical infrastructure
- National Coordinator for Security, Infrastructure Protection and Counter-Terrorism

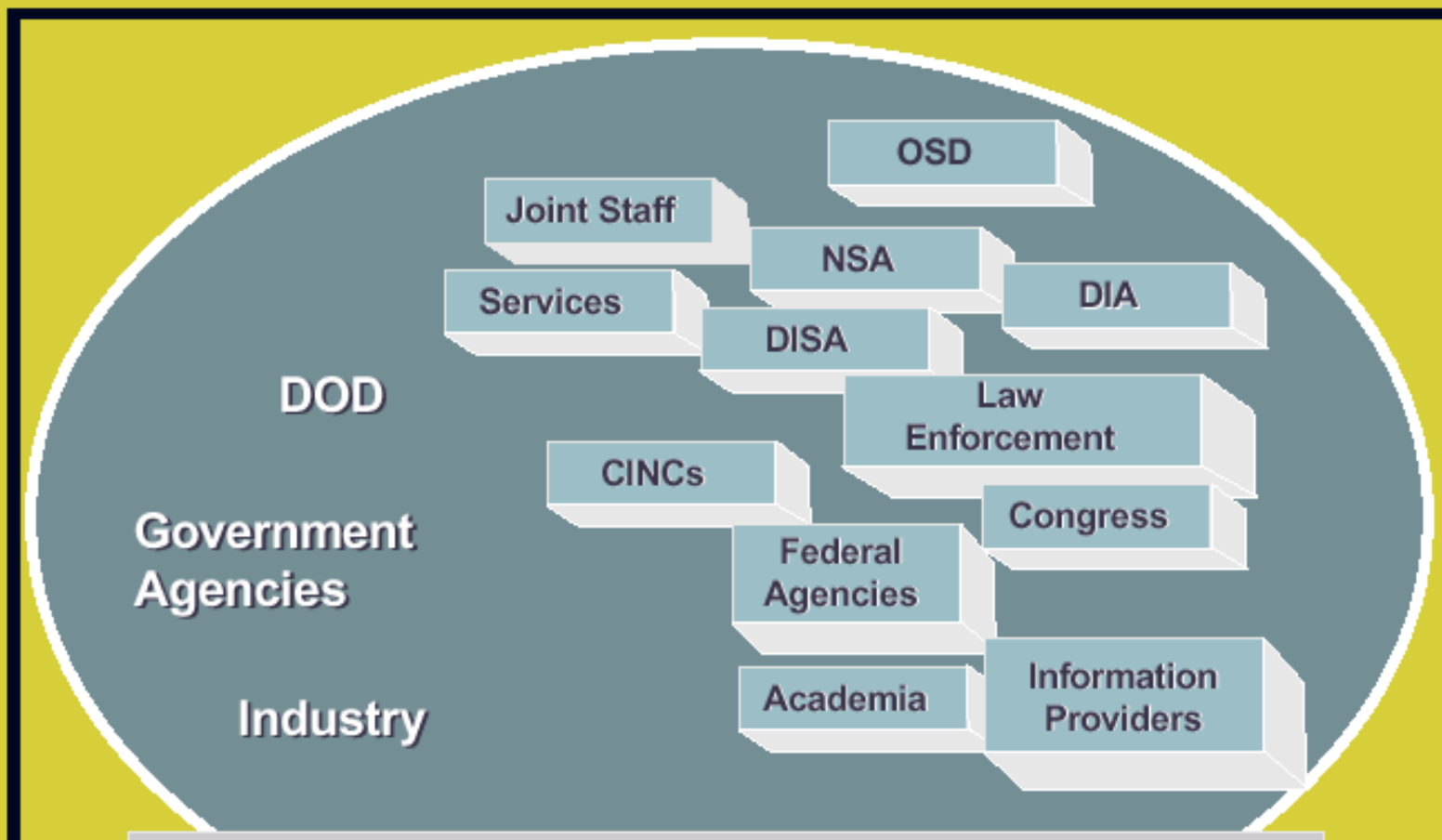
Presidential Decision Directive 63: Protecting America's Critical Infrastructures

CRITICAL INFRASTRUCTURE ASSURANCE OFFICE

- National Infrastructure Protection Center
  - DOJ / DoD/ FBI / CIA Response Protocols
    - Domestic threat/attack is a law enforcement concern
    - Foreign threat/attack could be a DoD / CIA concern
      - Difficulty in determining nature and level of a Foreign threat/attack
  - PDD 63 generally treats attacks or intrusions as criminal violations until evidence proves otherwise

Acrobat Reader - [jp3_13.pdf]
File Edit Document View Window Help

INFORMATION OPERATIONS PARTNERS



A teamed approach is essential to develop a comprehensive IO strategy

200% 25 of 136 6 x 9 in

Overview

- Relationship of Computer Crime (part of IA) to CNA
- Computer Crime Team
- Types of Computer Crime
  - Insider (military v. civilian)
  - Outsider
- Investigations
- Typical Scenerios

Substantive Crimes

Substantive Crimes

- Misuse of government computers
  - AFI 33-129, AFI 33-119
  - Article 92, UCMJ
- Identity Theft and Fraud, 18 U.S.C. 1028
- Espionage
  - Article 106a, UCMJ; 18 U.S.C. 1030
- Hacking: 18 U.S.C. 1030
- Obscenity: 18 U.S.C. 1462
- Child pornography
  - 18 U.S.C. 2252, 18 U.S.C. 2252A

Misuse of Government Systems

AFI 33-129, AFI 33-119; Article 92, UCMJ

File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit
Address http://afpubs.hq.af.mil/pubs/publist.asp?puborg=AF&series=33
Go Links

AFI33-117	18 May 1999	VISUAL INFORMATION (VI) MANAGEMENT	945K	HQ AFCIC/SYSM	
AFI33-118	01 Aug 1997	RADIO FREQUENCY SPECTRUM MANAGEMENT	379K	AFFMC/SCX	
AFI33-119	01 Mar 1999	ELECTRONIC MAIL (E-mail) Management and Use	453K	HQ AFCA/GCOM	
AFMAN33-120	01 Jun 1997	RADIO FREQUENCY (RF) SPECTRUM MANAGEMENT	2.3M	HQ AFFMA/SCX	
AFI33-122	01 Aug 1998	COMPUTER SYSTEMS MANUALS	51K	HQ SSG/SWCD	
AFI33-127	01 May 1998	ELECTRONIC MESSAGING REGISTRATION AND AUTHORITY	745K	HQ SSG/DI	
AFMAN33-128	01 Mar 1997	ELECTRONIC MESSAGING REGISTRATION	545K	HQ SSG/SI	
AFI33-129	01 Aug 1999	TRANSMISSION OF INFORMATION VIA THE INTERNET	46K	HQ AFCA/RMI	
AFI33-132	01 Dec 1998	ARMAMENT DELIVERY RECORDING PROGRAM	191K	HQ AFCIC/SYOT	
AFI33-202	01 Feb 1999	COMPUTER SECURITY	295K	HQ AFCA/GCI	
AFI33-203	01 May 1998	EMISSION SECURITY	289K	HQ AFCA/GCIS	

Internet

Misuse of Government Systems

AFI 33-129

Prohibitions:

- Any use of government-provided computer hardware or software for other than official and authorized government business
- Activities for personal or commercial financial gain
  - chain letters
  - commercial solicitations
  - sales of personal property

Misuse of Government Systems
AFI 33-129

- Storing, processing, displaying, sending, or transmitting obscene or offensive material
  - "hate literature"
  - sexually-harassing materials
  - pornography and sexually-explicit materials (includes "chat" rooms)
- Storing or processing classified on computer not approved for classified

Misuse of Government Systems

AFI 33-129

- Storing or processing copyrighted materials without approval from copyright owner
- Participating in “chat lines” or open forum discussions unless PA-approved
- Using another person’s account without permission
- Viewing, changing, etc. another’s files without permission

Misuse of Government Systems
AFI 33-129

- Attempting to circumvent or defeat security systems without permission
- Using software in violation of license agreement
- Permitting unauthorized access
- Modifying network without prior permission from administrator

Misuse of Government Systems
AFI 33-129

- Penalty: Violation of Article 92, UCMJ
- 2 years' confinement, DD, TF, E-1

Misuse of Government E-mail

AFI 33-119

- Punitive regulation effective 1 Mar 99
- Regulates official and authorized uses of government e-mail
  - Use of e-mail constitutes consent to monitoring and waives any right to privacy
  - E-mail is subject to the requirements of the Freedom of Information Act (FOIA)

Misuse of Government E-mail
AFI 33-119

- Differentiates between “official” and “authorized use”
- Establishes types of “authorized” use which can be made of government e-mail systems

- Penalties for violation (Art 92):
  - DD, 2 years’ confinement, E-1, TF

Identify Theft & Fraud

18 U.S.C. 1028

Identity Theft and Fraud
18 U.S.C. 1028

- Southern District of Florida. A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than $13,000 from the victim's bank account, and obtaining five department store credit cards in the victim's name and charging

Identity Theft and Fraud
18 U.S.C. 1028

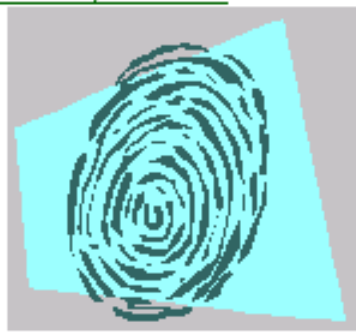
- 15 years imprisonment
- Fine
- Criminal forfeiture of any personal property used or intended to be used to commit the offense
- FBI, US Secret Service, US Postal Inspectors Service

Identity Theft and Fraud
18 U.S.C. 1028

- **Identification Fraud, 18 U.S.C. 1028**
- **Credit Card Fraud, 18 U.S.C. 1029**
- **Computer Fraud, 18 U.S.C. 1030**
- **Mail Fraud, 18 U.S.C. 1341**
- **Wire Fraud, 18 U.S.C. 1343**
- **Financial Institution Fraud, 18 U.S.C. 1344**
- **Felonies, up to 30 years imprisonment**

Identity Theft and Identity Fraud - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.usdoj.gov/criminal/fraud/idtheft.html
Go Links

Text Only Version



Identity Theft and Fraud

What Are Identity Theft And Identity Fraud?

What Are The Most Common Ways To Commit Identity Theft Or Fraud?

What's The Department Of Justice Doing About Identity Theft And Fraud?

What Can I Do About Identity Theft And Fraud?

- **What Should I Do To Avoid Becoming A Victim Of Identity Theft?**
- **What Should I Do If I've Become A Victim Of Identity Theft?**

Where Can I Find Out More About Identity Theft And Fraud?

Done
Internet
Start Inbox - ... Microsof... QuickTi... Identity ... Identit... 8:04 AM

Substantive Crimes

Espionage

Article 106a UCMJ

18 U.S.C. 1030

--The Insider Problem--
Spies Wanted:
No Skills, No Training Necessary

- The Spying Game Has Changed
  - No more dead drops, cut-outs, Leika cameras, microfilm, fat envelopes, long distance calls or trips to the Soviet Embassy
  - Today, you can betray your country from the comfort of your living room, or the “privacy” of your office
    - Steganography / Internet Chat Rooms / Web Pages
  - Computers hand decisive advantage to the offense because they promise *anonymity*
  - Aggregation of data
- But the Rules for Counterintelligence Haven’t!

STEGANOGRAPHY

Steganography, from the Greek word meaning secret, and the suffix - graphy writing or drawing.

Accomplished by hiding a small message in a larger message or object to prevent others from learning the secret.

"...Anyone carrying a single music cassette bought in a store could carry the entire computerized files of the stealth bomber, and it would be totally imperc

Tim May, The Crypto-Anarchist Manife

Price of Counterintelligence Failure

NATIONAL AFFAIRS

Open Secret

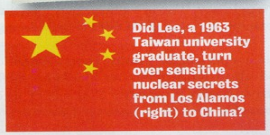
Forget about cloaks and daggers. In the nuclear age, China's playing a whole new espionage game.
BY DANIEL KLAIDMAN AND MELINDA LIU

IT LOOKED LIKE A CLASSIC SPY operation. Burrowed deep in Los Alamos, the mountaintop lab containing America's most sensitive nuclear secrets, a Taiwanese-born scientist, Wen Ho Lee, was suspected of passing classified-weapons specs to Beijing.

The news sent a shudder through official Washington. It was just the sort of national-security catastrophe that critics of the Clinton administration's China policy had been loudly predicting. Republicans, who had long accused the Clinton White House of cozying up to the Chinese government—sacrificing national security on the altar of commerce—demanded the resignation of National Security Adviser Sandy Berger. In the House, Republicans eager to score political points on foreign-policy issues prepared to release parts of a blistering 700-page report alleging a vast Chinese effort to spirit high technology out of the United States. The Lee case appeared to be a blueprint of how Beijing wages espionage.

A tantalizing story, to be sure. Was the gentle suburban scientist who made Peking duck for his neighbors actually a top Chinese operative? In the days since the Lee case was made public, a far less certain picture has emerged. Senior law-enforcement and intelligence officials tell NEWSWEEK that they are in fact not at all confident Lee passed on critical secrets to the Chinese—or even that espionage was involved at all. Lee was fired last week from his job at Los Alamos, but he has yet to be charged with any crime. The FBI now believes it has virtually no chance of making a case against him.

The fiasco painfully illustrates a disheartening truth for U.S. spy-catchers: the old tricks of the trade for tracking spooks may no longer be enough. The time-worn images of seasoned operatives making "dead drops" in dark alleys don't often apply to those caught helping Beijing. U.S. intelligence officials ac-



Did Lee, a 1963 Taiwan university graduate, turn over sensitive nuclear secrets from Los Alamos (right) to China?

FROM LEFT: AFP, GREG SMITH—SABA

'The Penetration Is Total'

CIA analysts find shocking evidence that Chinese spies have cracked even the most secret weapons labs

THE NEWS WAS WORSE than the CIA had imagined. Last week, in response to recent reports that China may have stolen nuclear secrets from Los Alamos and other U.S. weapons labs, President Clinton ordered a preliminary "damage assessment" to determine just how much Beijing knows about the American nuclear program. CIA analysts had already pulled together intelligence data gleaned from U.S. espionage against China and now began poring through it for clues. It wasn't easy. The material was rich in detail: it included years' worth of communications intercepts and revelations from a 1995 Chinese defector who worked on the Chinese nuclear program and spilled to his U.S. handlers. But most of the data had been languishing unread in intelligence-agency computers—for years. Some hadn't even been translated from Chinese.

NEWSWEEK has learned that when the CIA showed the material to a team of top nuclear-weapons experts, they "practically fainted." Chinese scientists routinely used phrases, descriptions and concepts that came straight out of U.S. weapons labs. "The Chinese penetration is total," says an official close to the investigation. "They are deep, deep into the labs' black programs."

U.S. officials believe that China may have acquired design information over the last two decades about seven U.S. nuclear warheads, including the neutron bomb created in the early 1970s. They may also have stolen secrets about U.S. efforts to devise a nuclear weapon tailored to create an electromagnetic pulse—a man-made lightning bolt that would short out anything in an enemy nation that uses electricity.

The government's damage-assessment team is now trying to figure out who could have given the secrets to Beijing. They do not believe it was a

CASE FILE: REMIS DATA BASE

SUBJECT: EMPLOYEE OF RED CHINESE SUB- CONTRACTOR

- 20NOV96 & 3DEC96 INTRUSIONS
- STOLE OPS SYSTEM PASSWORDS
- COMPROMISED GEN K'OR

SYSTEMS

- 5DEC96 GEN K'OR DISCOVERS
- 23DEC96 FAILED POLYGRAPH EXAM
- ARRESTED CHRISTMAS EVE

TIONALS WORK CT

STATUS: AFOSI / FBI JOINT INVESTIGATION CLOSED

SUBJECT PLED GUILTY TO BOTH CHARGES, SENTENCED ON 26 MAY 98 TO 6 MONTHS HALFWAY HOUSE AND $5,000 FINE

CONVICTION OVERTURNED, NEW TRIAL

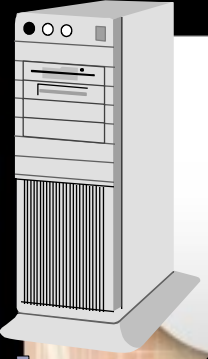
Moonlight Maze

- 'We're In The Middle Of A Cyberwar' *Russian hackers may have pulled off what could be the most damaging breach ever of U.S. computer security,* Newsweek, Sept. 20, 1999
- This was, Pentagon officials say flatly, "a state-sponsored Russian intelligence effort to get U.S. technology"

Hacker

18 U.S.C. 1030

The “Outsider” Problem



“. The modern thief can steal more with a computer than with a gun. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb. - National Research Council, “Computers at Risk: Safe Computing in the Info. Age,” 1991

“Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker.”

- President’s Commission On Critical

Hackers
18 U.S.C. 1030

Prohibitions:

- Obtaining restricted or classified U.S. government information
- Obtain information in a U.S. government computer
- Obtain a financial record
- Obtain information from “protected computer” in interstate commerce

Hackers
18 U.S.C. 1030

More prohibitions:

- Access computer used by U.S. government
- Access computer used in interstate commerce
- Causing transmission of program, code, etc., causing damage
- Trafficking in passwords
- Extortion

Hackers
18 U.S.C. 1030

Selected first offense penalties:

- Classified access: 10 years
- Obtain non-classified information, financial record, cause minor damage: 1 year
- Access for commercial advantage or private financial gain, in furtherance of crime, or value obtained more than $5,000: 5 years

Obscenity
Child Pornography

18 U.S.C. 1462

18 U.S.C. 2252

Article 134, UCMJ

Obscenity
18 U.S.C. 1462

Use of interactive computer service for:

- Any obscene, lewd, lascivious, or filthy book, pamphlet, picture, film, paper, letter, writing, print, or other indecent matter
- Any obscene, lewd, lascivious, or filthy phonograph recording, electrical transcription, or other sound-producer

Obscenity
18 U.S.C. 1462

- First offense: 5 years
- Subsequent offenses: 10 years

- Other obscenity laws: e.g., 18 U.S.C. 1465

Child Pornography
18 U.S.C. 2252

- Transportation, shipment, receipt, distribution, or sale in interstate commerce of visual depiction that
  - involves the use of a minor engaging in sexually explicit conduct, and
  - such visual depiction is of such conduct.
- Quantity
  - Prior to 30 Oct 98: 3 or more
  - After 30 Oct 98: 1 or more

Child Pornography
18 U.S.C. 2252

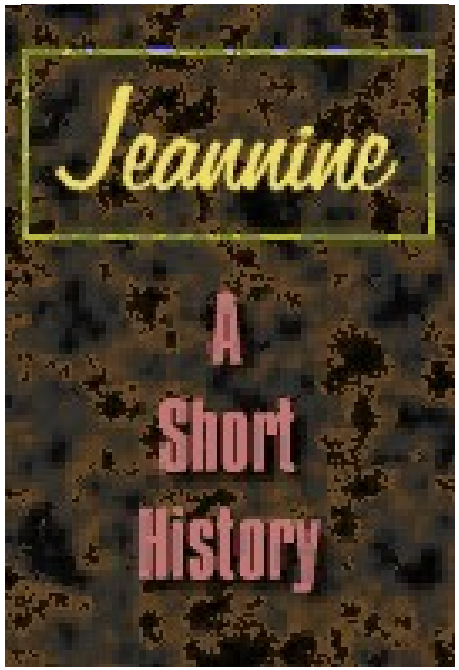
- Affirmative defense in some situations
  - Possess less than 3 matters containing prohibited images *and*
  - Promptly tried to destroy or report
- Penalty
  - Sale, transportation, etc.: 15 years
  - Simple possession: 5 years for first offense, 10 if prior sex offense

Child Pornography

Why is morphing important?

Child Pornography

Why is morphing important?



Child Pornography
18 U.S.C. 2252A

- Mail, ship, transport, reproduce, sell, or possess child pornography that has been in interstate commerce
- Possess book, magazine, periodical, film, etc., containing child pornography that has been shipped in interstate commerce or produced using materials that were shipped in interstate commerce

Child Pornography
18 U.S.C. 2252A
"Child pornography" defined.

- A visual depiction that:
  - used an actual minor engaging in sexually-explicit conduct in its creation;
  - is, or appears to be, of a minor engaging in sexually-explicit conduct;
  - has been created, adapted, or modified to appear that a minor is engaging in sexually-explicit conduct; or
  - is presented or advertised to contain a minor engaging in sexually-explicit conduct.

Child Pornography
18 U.S.C. 2252A

- Affirmative defenses in some situations
  - Possess less than 3 matters containing prohibited images *and* promptly tried to destroy or report
  - Image was created using an adult and not advertised as depicting a minor
- Penalty
  - Receive, distribute, reproduce: 15 years (30 if prior sex offense)
  - Simple possession: 5 years for first offense, 10 if prior sex offense

Child Pornography

Interrelationship between statutes

18 U.S.C. 2252

- **Minor must be used in the production of image**
- **“Morphing” provides complete defense**
- **Effective 6 Feb 78**

18 U.S.C. 2252A

- **Actual minor need not be used in the production of image**
- **“Morphing” no defense**
- **Effective 30 Sep 96***

* significant date is when crime was committed, not when image was created

Overview

- Relationship of Computer Crime
  - (part of IA) to CNA
- The Problem
- Computer Crime Team
- Types of Computer Crime
  - Insider (military v. civilian)
  - Outsider
- Investigations
- Typical Scenarios

When You'll See It…

- FBI/DOJ/OSI Investigation
  - U.S. Air Force personnel are implemented in a child pornography/fraud/hacker ring
- U.S. Customs Investigation
- Local Commander believes his troops are spending too much time on the computer
- Everything from Interpol to Amn Snuffy turning in his roommate

Who Handles What and When?
It Depends

- "Low level" Crime - JA, Commanders
  - (Ch 1 CCIH, pp 1-14 IOLH))
  - Art 15/Admin action type offenses can include misuse of govt computer to access adult porn to misuse for self-owned business purposes
  - Generally, OSI is out if its not Espionage, Hacker, or Child Pornography
    - They don't have the resources!
  - Comm Squadron is helpful in these scenarios combined with *commander directed inquiries or Security Forces*

Who Handles What and When?
It Depends…

- “Mid Level” Crime - JA, Commanders, SF
- Court-Martial Offenses (Ch 1 CCIH)
  - Repeated Misuse of Govt Computer Systems (AFI AFI 33-129, AFI 33-119
  - Profane/Obscene/Hate Crime Oriented/Unauthorized E-mail (AFI 33-129)
  - Sexual Harassment via the Internet has been prosecuted as well

Who Handles What and When?

It Depends…

- "High Level" Crime – AFOSI/DOJ
  - Court-Martial Offenses (Ch 6 CCIH)
    - Child Pornography, assisting U.S. Attorney (especially if civilian)
    - Child Pornography discovered through AF Investigation (military)
- "High Profile" Crime - Intruders/Hackers
  - (Ch 5 CCIH)
  - Hacker, Cracker, Phreaker, Phracker…
  - All *Intruders*
  - *Espionage*

Overview

- Relationship of Computer Crime
  - (part of IA) to CNA
- The Problem
- Computer Crime Team
- Types of Computer Crime
  - Insider (military v. civilian)
  - Outsider
- Investigations
- Typical Scenarios

Misuse of Government Systems
AFI 33-129

U.S. v. Monroe

(AFCCA Feb 5, 1999)

- Court found Monroe had no expectation of privacy in an e-mail account on a government server as to his supervisors and the system administrator (Banner)
- E-mail accounts were given for official business, although users were authorized to send and receive limited textual and morale messages to and from friends and family
- Monroe did not have a government computer, but had a personal computer in his dorm room

Monroe…

- Court used the analogy of an unsecured file cabinet in the member's superiors' work area in which an unsecured drawer was designated for his/her use in performing his/her official duties with the understanding that his superiors had free access to the cabinet, including the drawer
- Affirmed by CAAF, 13 March 2000

HOW DO WE CATCH THE HACKER or OTHER BAD GUY??

Information Security--Monitoring

- One of the first lines of defense in protecting AF information systems
- Monitoring performed for different reasons; by different actors
  - systems protection / network professionals
  - operational security / TMAP assets
  - evidentiary interception / law enforcement investigators

Restrictions to Monitoring

- 4th Amendment Right to Privacy
- Electronic Communications Privacy Act (ECPA)

Legal Principles--Constitutional Law

- **Fourth Amendment prohibition against Unreasonable Search & Seizure**
  - Protects people; not places
  - Is there a reasonable expectation of privacy?
  - If so, is the search reasonable?
    - Governed by totality of circumstances
    - Degree of protection proportional to expectation of privacy
    - Greater degree of intrusion = greater judicial supervision

EXPECTATION OF PRIVACY (Or, "We don' need no stinkin' warrant!")

- **Questions:**
  - **Who owns the computer?**
  - **Who owns the information on the computer**
  - **Who owns the e-mail file server?**
  - **Is there a banner on the computer?**
  - **What does the banner say?**
  - **Has the employee executed a written statement of understanding?**
  - **Do other people use computer?**
  - **Location of computer?**
  - **Are there periodic security checks?**
  - **Status of employee (active duty covered by MRE 314(d))**

Electronic Communications Privacy Act (ECPA)

- statutorily conferred an expectation of privacy in electronic and wire communications
- governs interception of electronic communications
- governs access into stored communications
- generally prohibits interception of electronic communications, or access into stored communications, without court order
  - aimed at law enforcement
  - numerous "exceptions"
    - including systems provider exception
    - consent

Information Security-- Monitoring Analysis

- Analysis starts with the three “Ws”
  - Who is monitoring?
  - What is being monitored?
  - Why is it being monitored?
- Different analytical blueprints based on purpose
  - Law Enforcement interceptions
  - Intel-counterintel surveillance
  - Systems protection monitoring
  - Other types of monitoring

Investigative Interception or Search Law Enforcement

- Consent
- Search Authorization / Warrant
- Distinction between 4th Amendment and ECPA

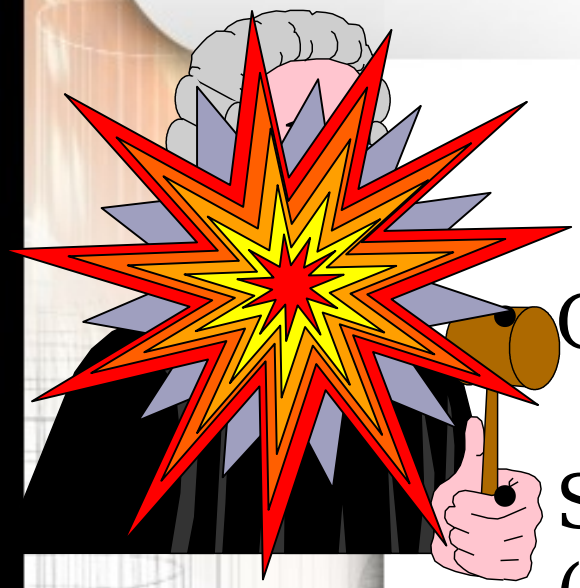
Interceptions

- DoDD 5505.9, 20 Apr 95
  - Establishes DoD O-5505.9-M as guide
  - Defines what agencies can conduct:
    - USACID
    - NCIS
    - AFOSI
    - DCIS
  - AFI 71-101, Vol. 1
    - AFOSI/CC Approval (Consensual only)
    - SAF/GC Approval for all Nonconsensual wiretaps

Tips on Handling Computer Abuse Cases

- SYSAD usually identifies govt. I.P. addresses where abuse taking place
  - *Does Not Need to Monitor Real-Time*
- Appropriate commander/senior leader should be briefed, then assemble all users to notify them of impropriety, warn
- If it continues, Sysad, commander, and SF can mount a “sting” to catch perp in the act

VIOLATIONS OF WIRETAP ACT / ECPA



Criminal 5 yrs + fine, PLUS

Statutory Exclusionary Rule (18 USC 2515), PLUS

- Civil Suit for Actual and Punitive Damages, Atty's fees, and court costs (18 USC 2520)

Hackers
18 U.S.C. 1030

LONDON DAILY TELEGRAPH March 23, 1997 Pg. 5

Hackers pillaged U.S. files to sell secrets to Saddam

TIM REID

HUNDREDS of military secrets, including troop movements and missile capability, were stolen from American government computers and offered to Saddam Hussein during the Gulf war, a former US security expert has admitted.

Computer hackers in the Netherlands used the Internet to steal enough top-secret information potentially to change the course of the war.

Luckily for the Allies, the Iraqis ignored the data, probably fearing a hoax, according to intelligence experts.

Dr Eugene Schultz, former head of computer security at the US Department of Energy, has disclosed for the first time how he and colleagues sat helpless as the Dutch hackers pillaged the files across 34 US military sites in the months leading up to the 1991 conflict.

space company. US military intelligence officials claimed he had caused "more harm than the KGB".

Pryce, of Colindale, north London, who was 16 at the time, was fined pounds 1,200.

Dr Schultz, who was also responsible for protecting the computers of US nuclear weapons sites, told the BBC that the Americans learnt for 90 that the ng offered g with the he source hoven. data was The Dutch the exact os and the they had. tion about capability American warships in the region.

"We realised that these files should not have been stored on Internet-capable machines," Dr Schultz said. "They related to our military systems, they related to Operation Desert Shield at the time, and later Operation Desert Storm. This was a huge mistake."

Once the Dutch hackers had gained access to a military computer site, they simply kept guessing different passwords until the system let them in. Once inside, they could pick and choose the exact information they wanted. The attacks lasted for months.

"We couldn't do anything about it," Dr Schultz said. "If we had shut down one machine that they had been getting into, they would have found others to launch the attacks from."

The full story of Iraqi involvement in this episode is still classified. The CIA will neither confirm nor deny that the hackers tried to sell military secrets to Iraq.

Solar
Sunrise

18 USC § 2703(d)

- 18 U.S.C. 2703(d) Court order to get subscriber records, identity, transactional logs--need showing of reasonable belief contents relevant and material to criminal investigation
- What you get with your court order
  - Connection Logs
    - Sending IP
    - Receiving IP
    - Times
    - Dates
    - And more

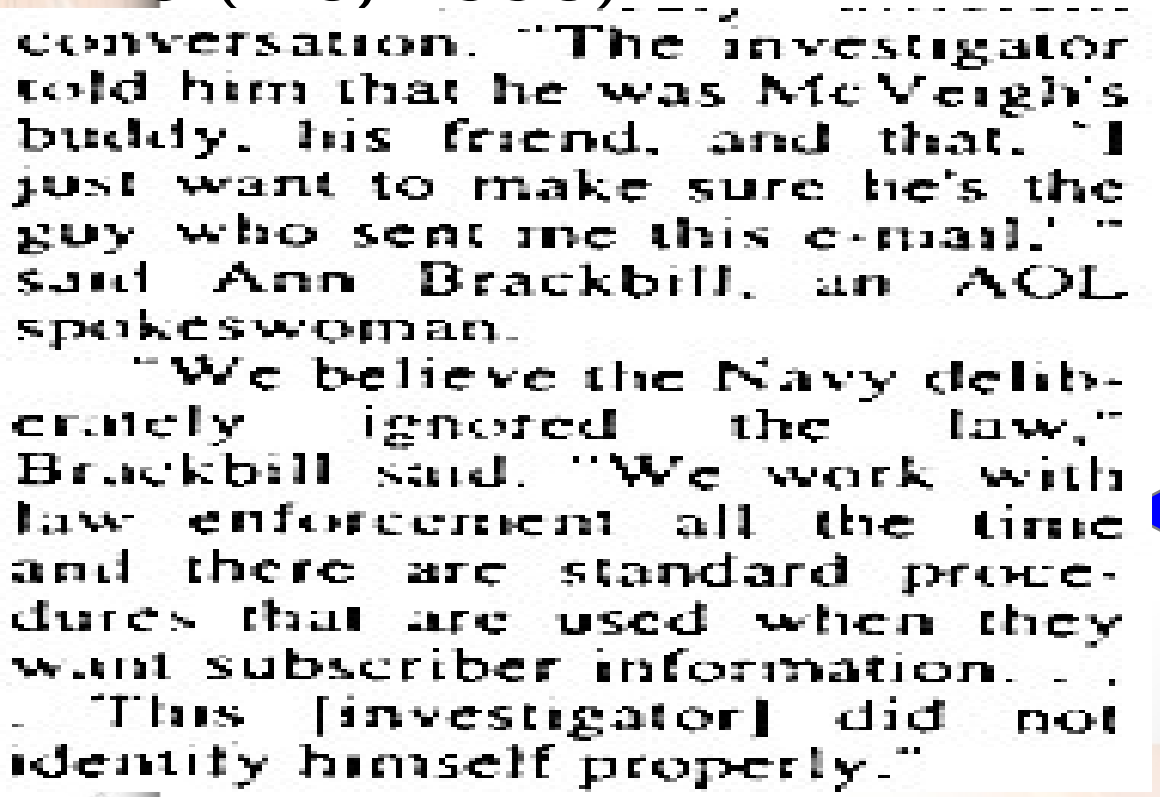
Violations of 2703

- Civil Liability 18 USC § 2707
- NO Criminal liability
- NO Statutory suppression
  - **Beware of Bad Faith argument**

LOOKS REAL BAD ON YOUR OPR!!!!

PITFALLS FOR THE UNWARY

- Subscriber Info, 18 USC 2703
  - *McVeigh v. Dept of Navy*, 983 F. Supp 215 (DC, 1998)

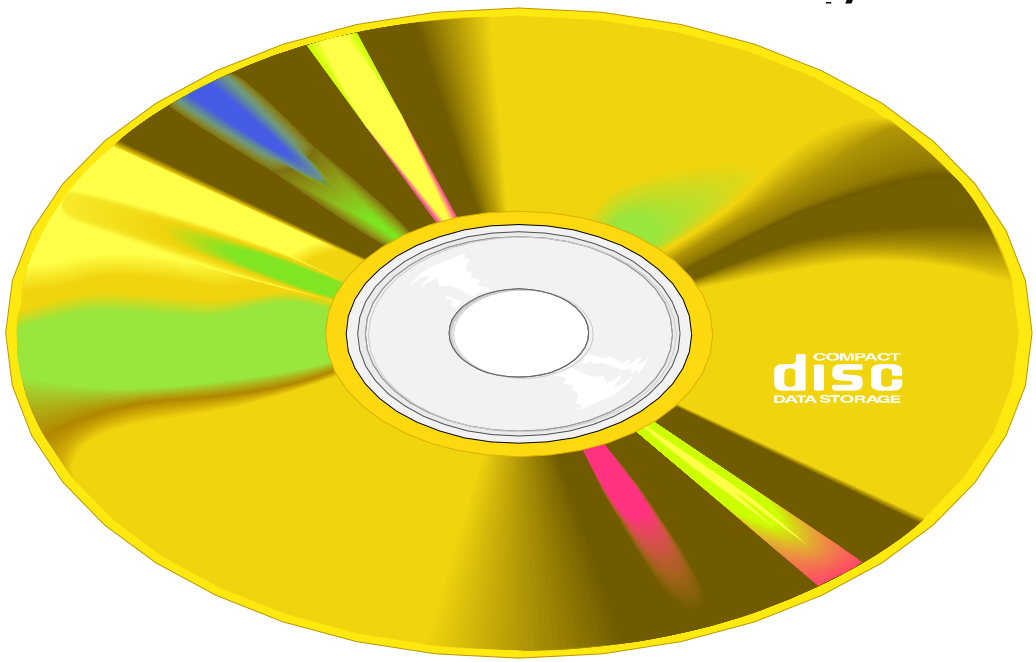


conversation. "The investigator told him that he was McVeigh's buddy, his friend, and that, 'I just want to make sure he's the guy who sent me this e-mail.' " said Ann Brackbill, an AOL spokeswoman.

"We believe the Navy deliberately ignored the law," Brackbill said. "We work with law enforcement all the time and there are standard procedures that are used when they want subscriber information. . . . This [investigator] did not identify himself properly."

Don't let this happen to you

- **Addition of 2703 (f)**
  - **Requires ISPs to hold data upon notification by law enfo ⊦ 90 day**



Child Pornography

18 U.S.C. 2252
Article 134,
UCMJ

U.S. v. Maxwell

45 M.J. 406, (CAAF 1996)

- Subjective expectation of privacy is question of fact (clearly erroneous standard)
- Whether subjective expectation is objectively reasonable is a matter of law subject to de novo review
- The transmitter of an e-mail message enjoys a reasonable expectation that the initial transmission will not be intercepted by the police without a warrant based on PC
- An expectation of privacy exists in e-mail transmissions made on an AOL service, however

On-Line Resources

- **HQ USAF/JAG: http://aflsa.jag.af.mil/GROUPS/AIR_FORCE/GENERAL_LAW/cyberlaw.htm**
- **Computer Emergency Response Team (AFCERT): http://www.cert.org/**
- **DOJ: http://www.usdoj.gov/criminal/cybercrime/**
- **FBI: http://www.fbi.gov/nipc/index.htm**
- **HQ USAF/AIA/JA http://aiaweb.aia.af.mil/homepages/ja/io_law.htm**
- **AFLSA/JAS, Law Tech 99: http://aflsa.jag.af.mil/flite/training/LTC99-1/**
- **Information Warfare Division, CADRE/WSW**

  http://132.60.140.10/warfarestudies/iwac/iwacpage.html

Relevant Directives (To name a few!)

- PDD 62, Combating Terrorism
- PDD 63, Critical Infrastructure Protection
- JP3-13, Joint Doctrine for Information Operations
- DoDD S 3600.1, Information Operations
- DOD Memorandum on Web Site Administration, 7 Dec 98
- DOD Memorandum on Communications Security and Information Systems Monitoring, 27 Jul 97
- AFDD 2-5, Information Operations
- AFPD 10-24, Air Force Critical Infrastructure Protection
- AFI 33-129, Transmission of Information via the Internet
- AFI 33-119, Electronic Mail Management and Use
- AFI 33-219, Telecommunications Monitoring and Assessment Program
- AFI 14-104, Intelligence Oversight
- TJAG Policy Letter 31, Legal Information Services